CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Tallinn 2022

EXECUTIVE SUMMARY OF

Military Movement: Risks from 5G Networks

Executive Summary of Military Movement: Risks from 5G Networks

This research report examines a potential NATO military movement scenario for 2030 and its associated interactions with 5G technology in the areas of seaports and road transportation. It discusses the benefits the movement scenario could reap from 5G technologies and use cases in place by 2030. A more in-depth discussion follows, looking into the technological constitutions of these use cases and the corresponding risks as well as risk mitigation measures. The report aims to raise awareness among decision makers about how the quick development of 5G in the commercial setting will interact with military movement and result in strategic decisions the Alliance will need to make to avoid being caught off guard. To that end, it gives an evidence-based overview of the technological aspects of the relevant 5G development as well as a framework for mitigating the resulting risks.

The military movement scenario discussed takes place in 2030 and is premised on Russia and Belarus beginning to assemble large numbers of units close to their borders with Lithuania, Latvia, and Estonia. As a response to the growing threat to NATO territory, the Alliance decides to militarily reinforce the Baltic region. In what is a peacetime movement in nature, units are deployed forward from various allied NATO countries, including the US, Germany, Italy, and the UK. Personnel, vehicles, and containerised loads are moved both by strategic movement channels (by air and sea) as well as operational movement channels (by rail and road). Based on the smart seaport and smart road use cases selected as the focus of the report, focus is restricted to the movements by sea and road. Mostly civilian-owned infrastructure, equipment and services are used to enable the movements, which implies that the main 5G technology enablers (5G Radio Spectrum Allocation, 5G Core Network and Proximity Services), as well as the use cases, were incentivised by and developed for commercial purposes.

By 2030, important commercial seaports in Europe will have fully embraced 5G-enabled solutions, hence becoming 'smart'. The new 5G use cases in those ports will include, for instance, remote-controlled ship-to-shore cranes, automated guided vehicles, and drones for surveillance and inspection. These use cases have been enabled by the transformation of seaport connectivity solutions from the fragmented legacy systems of old to a more reliable and resilient consolidated 5G network that has security by design and performance characteristics optimised for the Internet of Things (IoT). The technological architecture of a smart seaport follows the typical IoT-edge-data centre / multi-access edge computing (MEC) approach but has characteristics unique to this environment such as a 'fixed' set of systems relating to the physical infrastructure (cranes, cameras) and the dynamicity of the system as smart elements such as containers and ships with private on-board networks are required to join the smart port network and communicate with smart port systems. In the context of this architectural setup, employing 5G private networks is the key to achieving an optimal balance between maximising benefits and minimising risks. As the military interacts with smart seaports in 2030, it will to some extent benefit from the increased efficiency, throughput, reliability, and security they offer. The benefit, however, is limited as the operational efficiency improvements offered are not so relevant to military movements for which the biggest bottlenecks are related to limited physical capacity to clear the cargoes for onwards movement from ports to their final destination. On the other hand, and more importantly, the Alliance will have to be mindful of the risks that the interaction introduces, for example, make sure the image-based data that the various portside cameras and devices gather would not be

propagated outside of the seaport private network, including physical data storages.

In addition to smart seaports, the military will heavily rely on road transportation for the operational movement of military assets. Road transportation and its value chain tie in with the future of military movement scenarios that will heavily rely on novel intelligent transportation system (ITS) technologies, which allow for the optimisation and cost-effectiveness of the logistical processes. With the continuous roll-out of 5G networks in Europe, the transportation sector will gradually shift to using more intelligent solutions. With 5G use cases in road transportation, the vehicles will form a platoon (tight convoy) and move in unison while gathering and using information from different road and transportation solution users. One of the most important enablers for further ITS services is cellular vehicle to everything (C-V2X) communication, which creates a system of hard real-time situational awareness about all parties involved in traffic. The overall idea of V2X is to enable real-time information sharing between vehicles, react to changing traffic and road conditions in a timely way according to road sensors, safely collaborate with vulnerable road users (VRUs), i.e. pedestrians and cyclists, and more. C-V2X with its low latency and high reliability is perfect to address road safety, fuel economy – especially for heavy vehicles – and overall traffic efficiency. Future military transportation should be more efficient, smoother, and more environmentally friendly.

Compared to the seaport use case, which will involve a private/hybrid network with extra security, V2N services for smart road transportation will rely on the existing public cellular network infrastructure to be continuously upgraded for 5G-driven novel services. Due to setup costs, it would be unrealistic to operate road transportation in a separate private network, therefore, the military needs to rely on public networks covering the major transportation routes in different countries, depending on the destination, taking into account relevant cybersecurity risks. For conventional civil use cases, shared multi-access edge computing (MEC) computing will be enabled for computationally demanding and shared tasks. The MEC solution is used to operate and manage the V2V and V2N systems. As for the smart ports, interacting with smart transportation solutions can bring an upside and opportunities for the military, but the Alliance will have to be mindful of the cybersecurity-related risks that the interaction and dependency on MEC introduces.

When relying on MEC technology, a variety of risks that are separate from generic 5G network-related risks need to be addressed to ensure a high level of security. Both use cases are a critical part of the infrastructure for logistics with high demands for data security and to protect the military assets being transported. With potential malicious behaviour from third-party attacks and threats that can be directly linked to the vehicles and equipment used for the transportation of military assets, risk mitigation needs to be fulfilled at every stage of the value chain and certain types of risks that can harm the systems, monitor asset movements, or even damage the assets, need to be evaluated. Therefore, cybersecurity solutions require collaboration between different actors and an understanding of the system and data flows not only between automated equipment but also to sensors, site operations centres and control centres for remote management and tele-operations. For cybersecurity related MEC risks, the report provides three main guidelines to follow to ensure the safety of the procedures and to lower risk. These main risk mitigation measures are compliance with global security standards, mitigation through end-to-end security management, and securing the digital infrastructure's supply chain.

The report concludes by emphasising that it is essential for cybersecurity management that security comes first, in relation to people, processes, and technologies. This requires specific operational technology, cybersecurity practices and adapted design characteristics for the solutions. Three sets of recommendations are made to the military and the policymakers. First, regarding policies and standards, is to pursue closer cooperation among the like-minded nations, including harmonisation of 5G-related policies and standards across NATO and EU member states. Second, regarding the mitigation of risks

related to system architecture, the interested parties, most notably NATO in close cooperation with the EU, must be (1) proactive in planning by developing a comprehensive 5G cybersecurity strategy; (2) engaged in building secure systems and 5G networks from the start by providing guidelines to commercial partners on the military-related security needs; and (3) stringent in security monitoring and enforcement by developing and communicating a set of system architecture requirements that the commercial partners are strongly encouraged to follow. Moreover, this report lists cybersecurity-related risks and mitigation measures, which can serve as a basis for auditing the implementation of 5G solutions for military movement. Regarding use cases, the report (1) recommends a close collaboration with the seaports that are critical for military movement and advocates setting up proprietary closed private 5G networks that are separate from the public 5G infrastructure or, at least, use the advantages of network slicing provided by 5G technology; and (2) acknowledges that smart road transportation will heavily rely on less secure 5G public networks, thus imposing restrictions on military movement, which can, however, be mitigated by certain technical and regulative measures. Finally, it is suggested that a multinational and cross-organisational (military–private sector interaction) pilot programme be created to address the co-development of 5G systems and associated challenges.

This research report is the second report from the CCDCOE 5G Supply Chain and Network Security research project.